Penetration Test Report: OWASP Juice Shop

Test Date: April 18, 2025
Tester: Kacper Waliczek
Target: OWASP Juice Shop (localhost:3000)
Environment: Node.js web application, HTTP/HTTPS

Executive Summary

This penetration test, conducted on April 18, 2025, identified two critical vulnerabilities in OWASP Juice Shop that require immediate attention:

- **Privilege Escalation (VULN-001, Critical)**: Attackers can gain administrative access, compromising the entire system.
- **CAPTCHA Bypass (VULN-002, High)**: Automated feedback submissions can flood the application with malicious content.

Business Impact if Unresolved:

- Data breaches exposing sensitive user information.
- Reputational damage from spam or fraudulent feedback.
- Potential legal and financial penalties.

Recommendations:

- Implement server-side validation for user roles and CAPTCHA responses.
- Apply rate-limiting to feedback submissions.
- Conduct regular security assessments.

For a detailed technical analysis, refer to the sections below.

Vulnerability Summary

ID	Vulnerability	CVSS Score	Severity
VULN-001	Privilege Escalation via Registration	9.1	Critical
VULN-002	CAPTCHA Bypass via Automated Feedback	8.2	High

Chart 1: Vulnerability Distribution by Severity

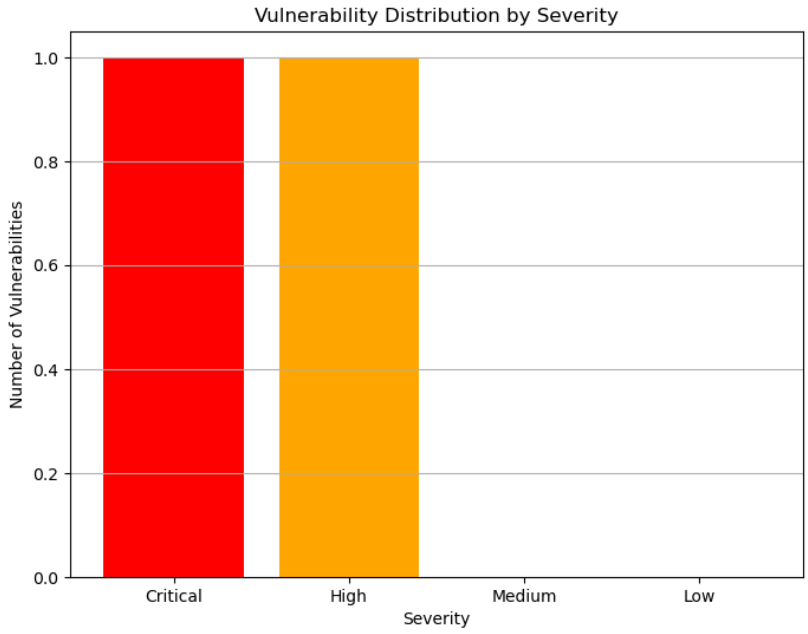
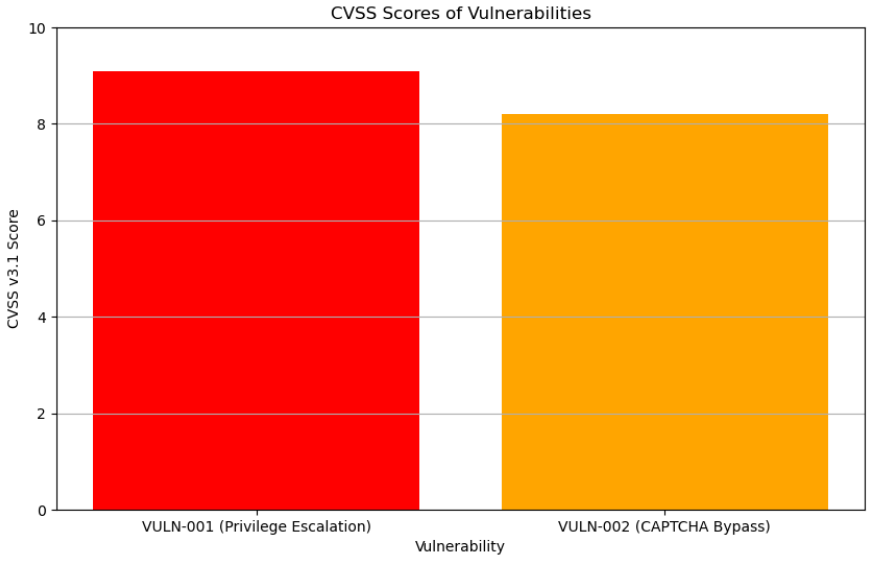


Chart 2: CVSS Scores of Vulnerabilities



Findings

Critical Severity

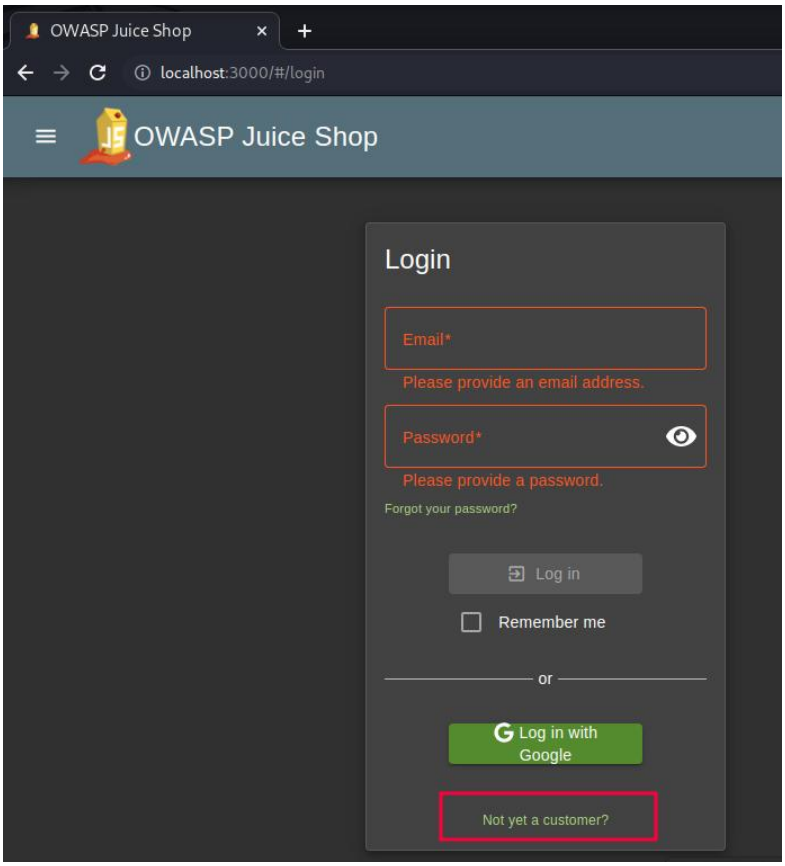
VULN-001: Privilege Escalation via User Registration

- CVSS Score: 9.1
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

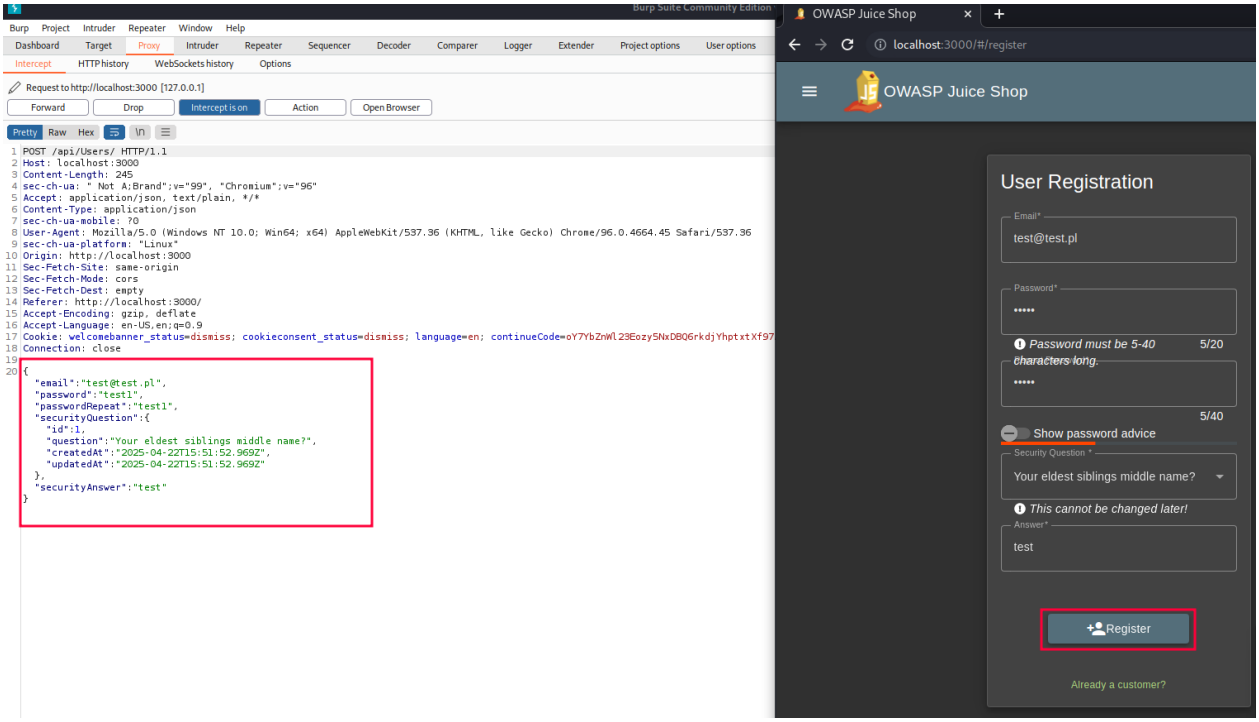
Description: The /api/Users/ endpoint allows attackers to set the role to admin during registration, granting full administrative access without verification.

Proof of Concept:

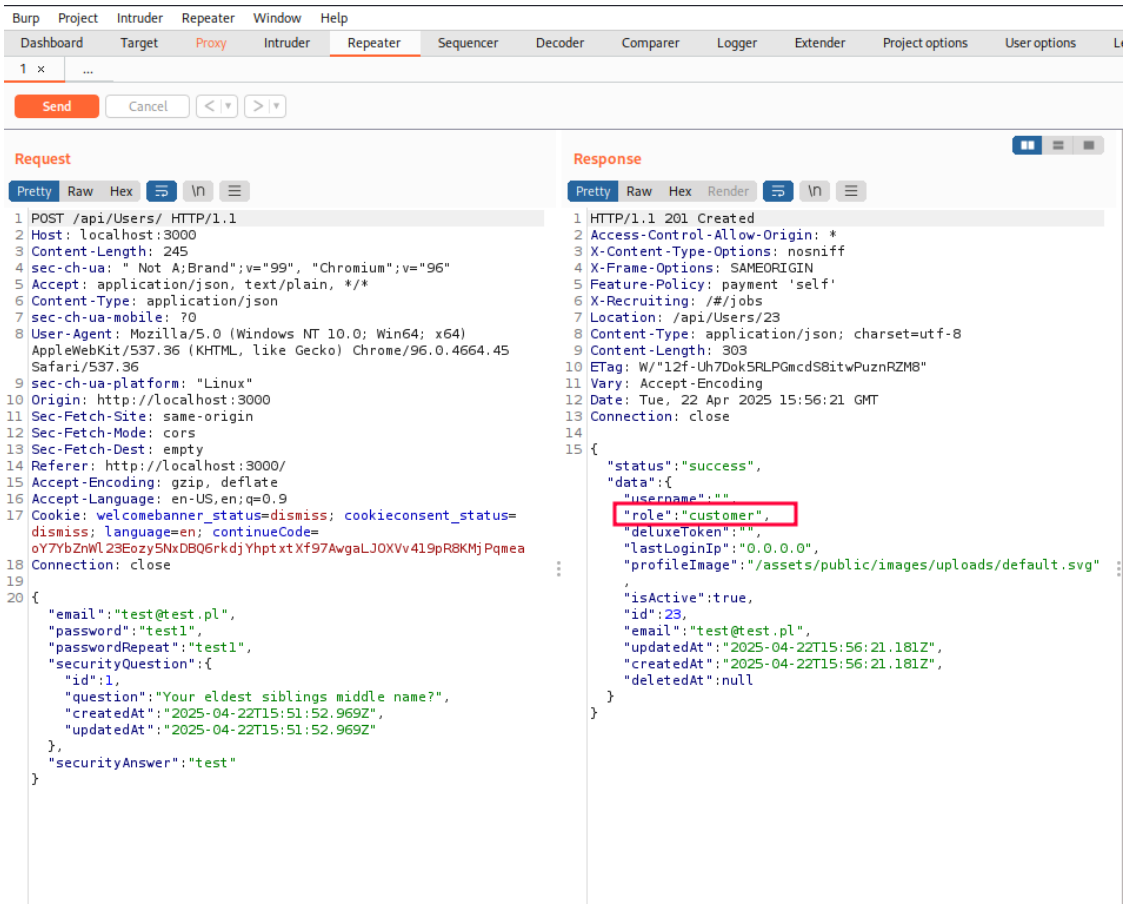
1. Visit localhost:3000/#/register.

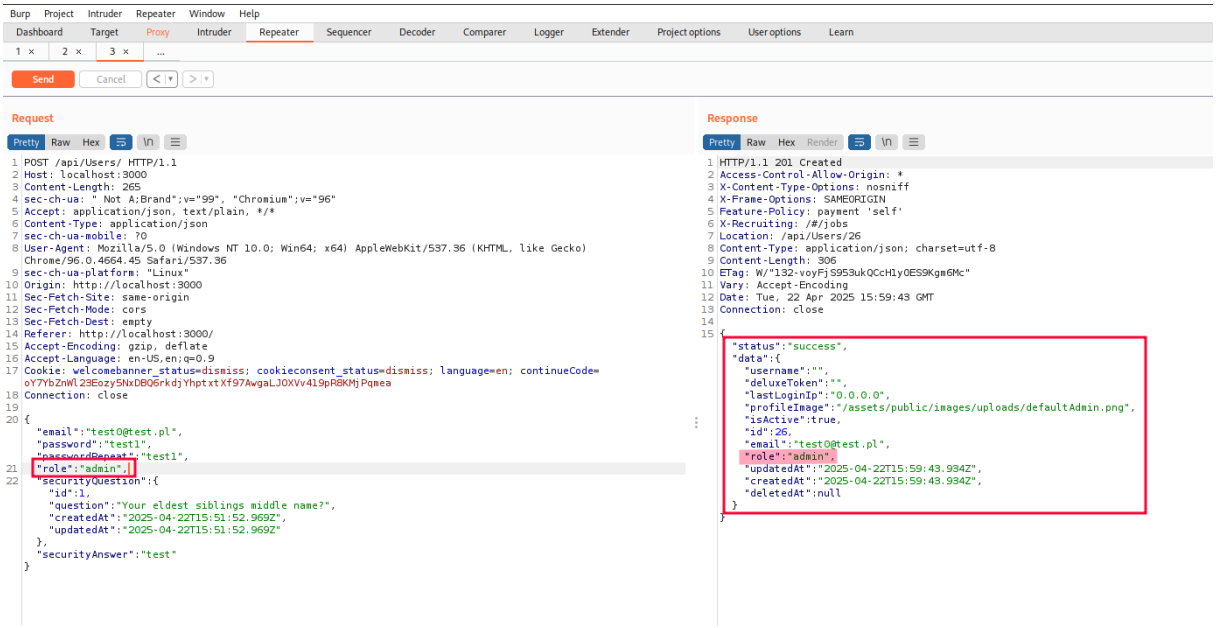


2. Submit registration details (e.g., email, password, security question).

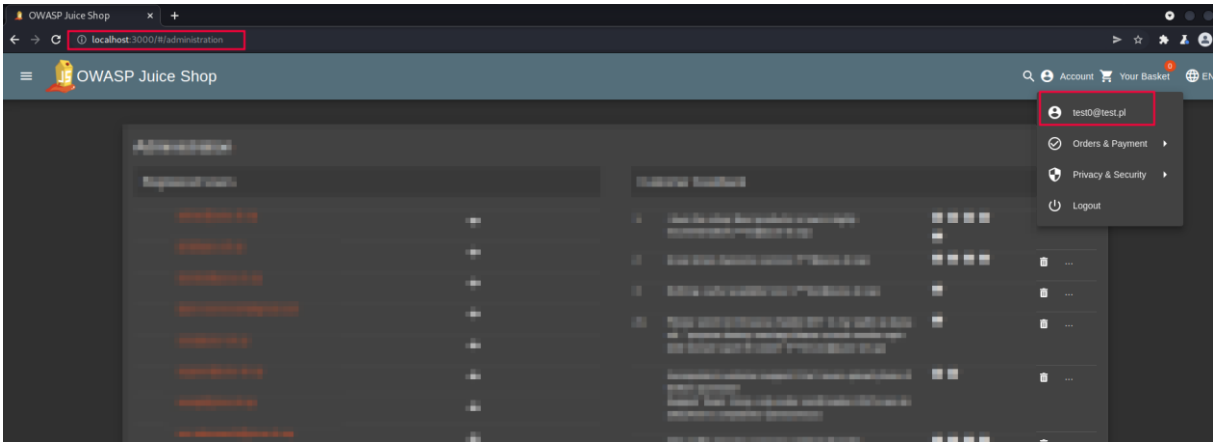


3. Use Burp Suite to modify the role to admin.





4. Confirm admin access by logging in.



Impact:

- Complete system control, enabling data theft or service disruption.
- Unauthorized changes to users or application settings.

Mitigation:

- Validate role server-side, enforcing customer.
- Restrict admin roles to secure, authenticated endpoints.
- Add CSRF tokens to registration forms.
- Log role assignments for monitoring.

High Severity

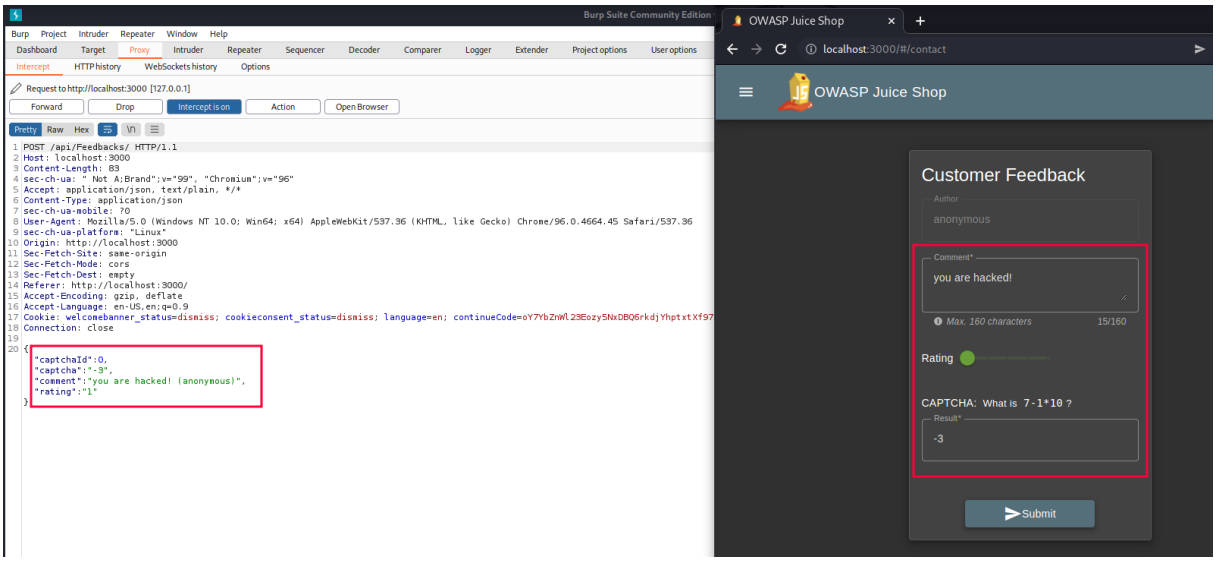
VULN-002: CAPTCHA Bypass via Automated Feedback

- CVSS Score: 8.2
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

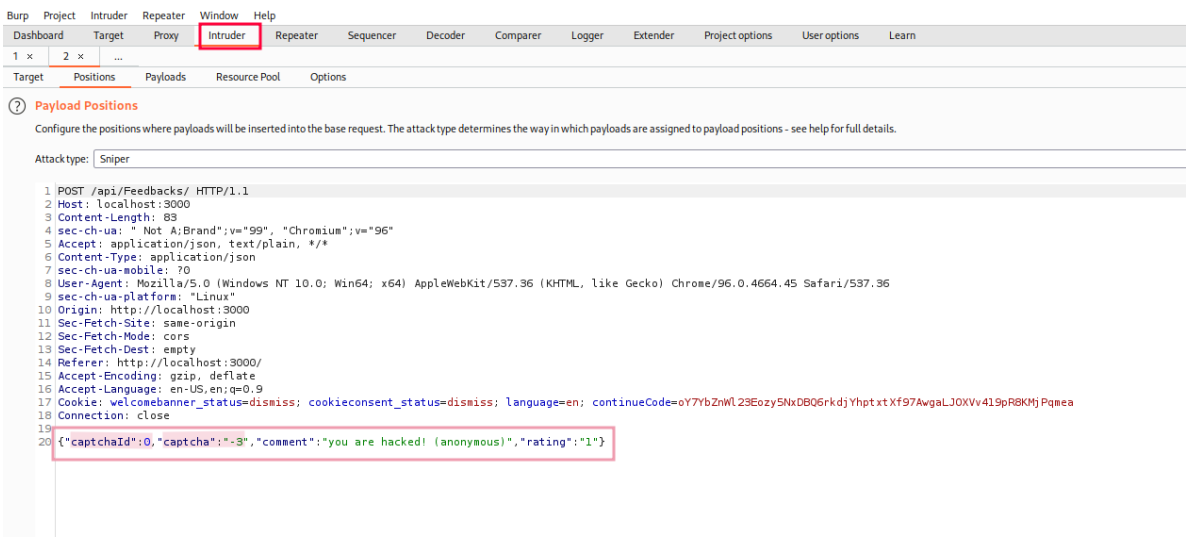
Description: The /api/Feedbacks/ endpoint's static CAPTCHA allows attackers to automate feedback submissions, bypassing verification.

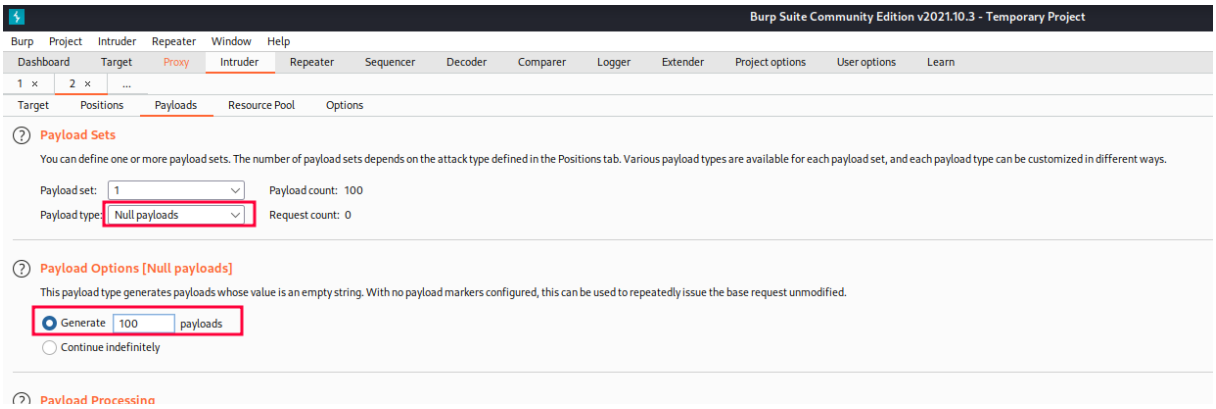
Proof of Concept:

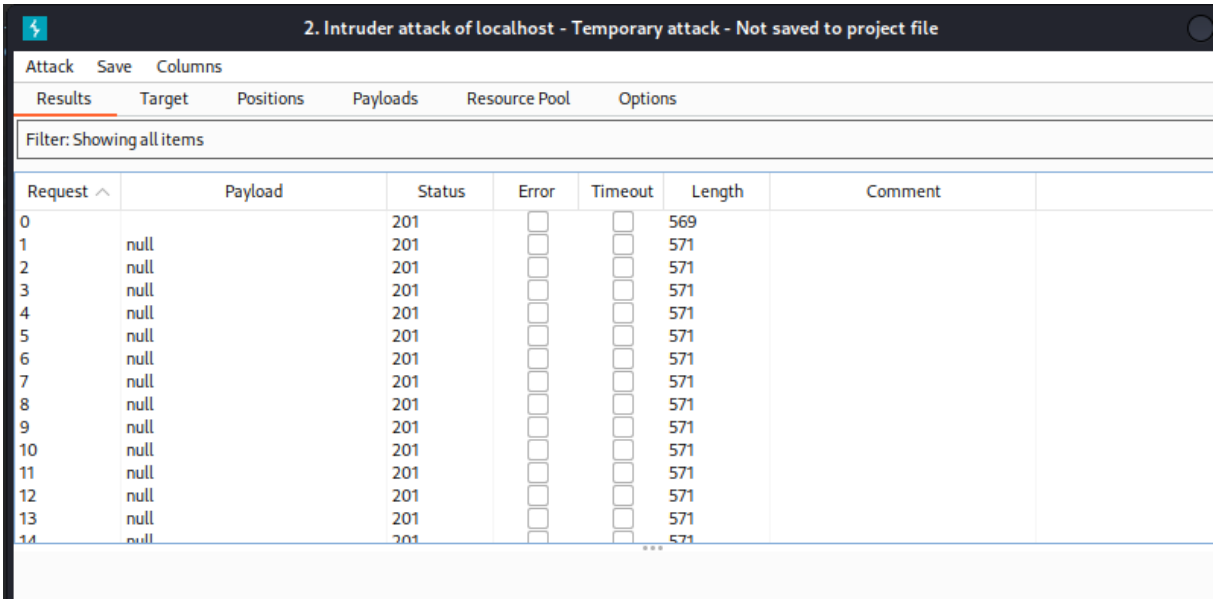
1. Visit localhost:3000/#/contact.
2. Submit feedback with a known CAPTCHA answer.



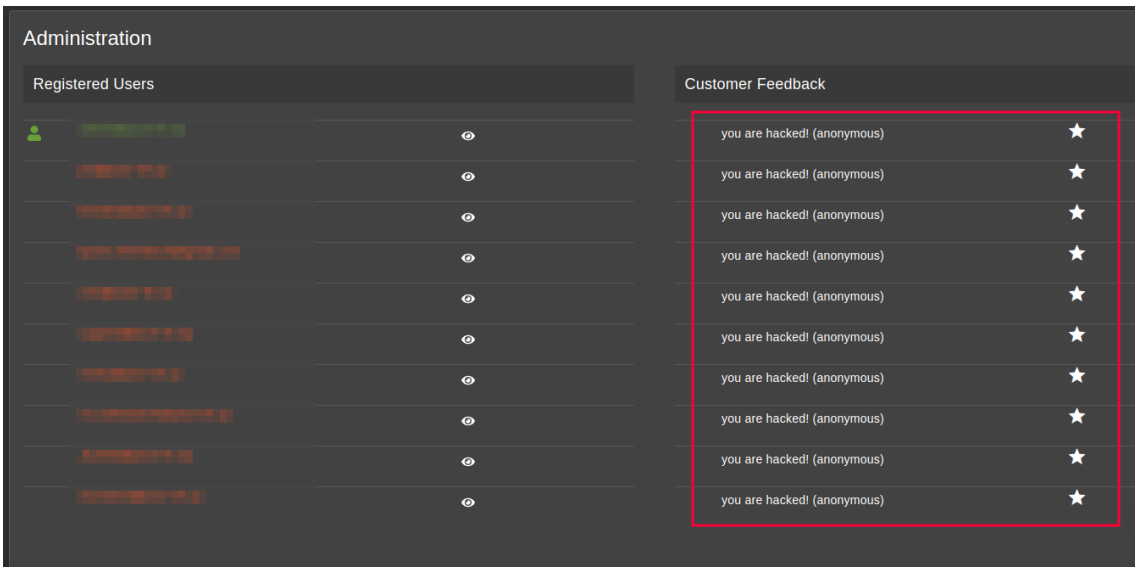
3. Use Burp Suite Intruder to repeat the submission.







4. Verify multiple feedback entries.



Impact:

- Spam or malicious feedback, harming application credibility.
- Potential for phishing or harmful content.

Mitigation:

- Implement dynamic CAPTCHAs per session.
- Validate CAPTCHA responses server-side, invalidating reuse.
- Apply rate-limiting (e.g., 5 submissions/hour/IP).
- Sanitize feedback content.

Medium Severity

- No medium-severity vulnerabilities identified.

Low Severity

- No low-severity vulnerabilities identified.

Remediation Summary

Recommendation	Priority	Vulnerability
Server-side role validation	Critical	VULN-001
CSRF tokens for registration	Critical	VULN-001
Dynamic CAPTCHAs	High	VULN-002
Rate-limiting on feedback	High	VULN-002
Feedback input sanitization	High	VULN-002

Recommendations

- Immediate Actions:
    - Fix VULN-001 with server-side role validation and CSRF tokens.
    - Address VULN-002 with dynamic CAPTCHAs and rate-limiting.
- Long-Term:
    - Test the application quarterly for new vulnerabilities.
    - Validate all API inputs to prevent manipulation.
    - Update Node.js and dependencies regularly.

Conclusion

OWASP Juice Shop is exposed to critical and high-severity vulnerabilities that could lead to system compromise or reputational damage. The charts and screenshots highlight the urgency of these issues. Implementing the recommended fixes will enhance security. Contact me for further clarification.

Prepared by: Kacper Waliczek